

This Page Is Inserted by IFW Operations  
and is not a part of the Official Record

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning documents *will not* correct images,  
please do not report the images to the  
Image Problem Mailbox.**

IN THE CLAIMS:

Please amend claims 1-14 and 16-20, and add new claims 21-28 as follows:

1           1.     (Currently Amended) A storage medium data protecting  
2     method of protecting data on a storage medium having a plurality of unit storage  
3     areas, comprising:

4                 a step of generating a random key ~~data~~, encrypting ~~the~~ said random  
5     key ~~data~~ with a password, and writing ~~the~~ said encrypted random key ~~data~~ to ~~said~~  
6     the storage medium;

7                 a step of encrypting the data with the generated random key ~~data~~,  
8     and writing the encrypted data to ~~said~~ the storage medium;

9                 a step of reading ~~the~~ said encrypted key ~~data~~ from ~~said~~ the storage  
10    medium;

11                a step of decoding ~~the~~ said encrypted key ~~data~~ with ~~the~~ said  
12    password; and

13                a step of reading and decoding the data on ~~said~~ the storage medium  
14    with the decoded key ~~data~~,

15                wherein said random key ~~data~~-generating step comprises:

16                a step of generating a different random key ~~data~~ for each of ~~a~~  
17    ~~plurality of unit storage area of the plurality of unit storage areas of said storage~~  
18    ~~medium, so that said each unit storage area is assigned a different random key, and~~  
19    said assignment of said different random key to said each unit storage area being

20 based on a particular unit storage area to which the data, once encrypted, is to be  
21 stored;

22 a step of encrypting each ~~said~~ of the different random key data for  
23 ~~each unit storage area~~ keys with said password, and

24 a step of writing each ~~said~~ of the encrypted key data to ~~said~~ different  
25 random keys to the storage medium when initializing the storage medium,

26 wherein said data encrypting step comprises a step of encrypting the  
27 data with ~~the~~ said different random key data corresponding to its said particular  
28 unit storage area to write the data, and

29 wherein said data decoding step comprises a step of decoding the  
30 data with ~~the~~ said decoded key data corresponding to said particular unit storage  
31 area where the data have been read.

1 2. (Currently Amended) A storage medium data protecting  
2 method according to claim 1, wherein said random key data-generating step  
3 comprises a step of generating ~~the~~ said random key data-per logic sector on said  
4 the storage medium.

1 3. (Currently Amended) A storage medium data protecting  
2 method according to claim 1, wherein said random key data-generating step  
3 comprises a step of generating ~~is different key data~~ random keys for each writing  
4 to said plurality of unit storage areas.

1                   4.     (Currently Amended)     A storage medium data protecting  
2 method according to claim 1, wherein said random key data-generating step  
3 comprises a step of generating ~~the key data~~ said random keys by combining a  
4 predetermined number of pieces of random data.

1                   5.     (Currently Amended)     A storage medium data protecting  
2 method according to claim 1, further comprising:

3                   a step of decoding, after reading ~~the~~ said encrypted key data from  
4 ~~said~~ the storage medium, ~~the~~ said encrypted key data with an old password  
5 designated by a user; and

6                   a step of writing, after encrypting ~~the~~ said decoded key data with a  
7 new password designated by ~~the~~ said user, the encrypted key data to ~~said~~ the  
8 storage medium.

1                   6.     (Currently Amended)     A storage medium data protecting  
2 method according to claim 1, wherein said ~~step of writing the~~ said encrypted  
3 random key data to ~~said~~ the storage medium comprises a step of encrypting the  
4 said random key data with each of a plurality of passwords, and writing ~~the~~ said  
5 encrypted random key data ~~keys~~ to ~~said~~ the storage medium, and said step of  
6 decoding the encrypted key data comprises a step of decoding ~~the read/encrypted~~  
7 ~~data~~ said encrypted key with a ~~password~~ designated password.

1                   7.     (Currently Amended) A storage medium data protecting  
2 method according to claim 1, wherein said ~~step of writing the said encrypted~~  
3 random key data to said ~~the~~ storage medium comprises a step of encrypting the  
4 said random key data with a first password, writing the encrypted random key data  
5 to said ~~the~~ storage medium, encrypting said first password with a second  
6 password, and writing said ~~first the~~ encrypted first password to the storage  
7 medium, and said step of decoding the encrypted key data comprises a step of  
8 decoding said ~~first~~ encrypted first password with said second password, and  
9 obtaining said first password, and a step of decoding the ~~said~~ encrypted key data  
10 with obtained said first password.

1                   8.     (Currently Amended) A storage medium data protecting  
2 apparatus for protecting data ~~on a storage medium~~, comprising:  
3                   a storage medium having a plurality of unit storage areas; and  
4                   a control circuit for reading and writing the data from and to said  
5 storage medium,  
6                   wherein said control circuit has:  
7                   a write mode of encrypting, after generating a random key data, the  
8 said random key data with a password, writing the encrypted key data to said  
9 storage medium, encrypting the data with the random key data, and writing the  
10 encrypted data to said storage medium;

11 a read mode of ~~encoding~~ decoding, after reading the ~~said~~ encrypted  
12 key ~~data~~ from said storage medium, the encrypted key ~~data~~ with the ~~said~~  
13 password, and decoding the data on said storage medium with the decoded key  
14 ~~data~~,

15 wherein said write mode comprises a mode of generating a different  
16 random key ~~data~~ for each unit storage area of said ~~storage medium~~ plurality of unit  
17 storage areas so that said each unit storage area is assigned a different random key,  
18 and the assignment of said different random key to said each unit storage area  
19 being based on a particular unit storage area to which the data, once encrypted, is  
20 to be stored, encrypting each ~~said~~ of the different random key ~~data~~ for each unit  
21 storage area keys with said password, writing each ~~said~~ of the encrypted key ~~data~~  
22 keys to said storage medium when initializing the storage medium, and encrypting  
23 the data with the random key ~~data~~ corresponding to its said particular unit storage  
24 area to write the data,

25 wherein said read mode comprises a mode of decoding the data with  
26 the decoded key ~~data~~ corresponding to said particular unit storage area where the  
27 data have been read.

1 9. (Currently Amended) A storage medium data protecting  
2 apparatus according to claim 8, wherein said storage medium is constructed of a  
3 storage medium from and to which the data is read and written per logic sector,

4 and said control circuit generates ~~the said different random key data~~ per logic  
5 sector on said storage medium.

1 10. (Currently Amended) A storage medium data protecting  
2 apparatus according to claim 8, wherein said control circuit generates different key  
3 ~~data-random keys~~ for each writing to said plurality of unit storage areas.

1 11. (Currently Amended) A storage medium data protecting  
2 apparatus according to claim 8, wherein said control circuit generates ~~the key data~~  
3 said different random keys by combining a predetermined number of pieces of  
4 random data.

1 12. (Currently Amended) A storage medium data protecting  
2 apparatus according to claim 9, wherein said control circuit decodes, after reading  
3 ~~the said~~ encrypted key data from said storage medium, ~~the said~~ encrypted key data  
4 with an old password designated by a user, and writes, after encrypting ~~the said~~  
5 decoded key ~~data~~ with a new password designated by the user, ~~the said~~ encrypted  
6 key ~~data~~ to said storage medium.

1 13. (Currently Amended) A storage medium data protecting  
2 apparatus according to claim 8, wherein said control circuit has:

3                   a write mode of encrypting ~~the key data~~ said random keys with each  
4   of a plurality of passwords and writing the encrypted ~~key data~~ keys to said storage  
5   medium; and  
6                   a read mode of decoding the read/encrypted key ~~data~~ with the a  
7   designated password.

1                   14.   (Currently Amended)       A   storage   medium   data  
2   protecting apparatus according to claim 8, wherein said control circuit has:

3                   a write mode of encrypting ~~the said~~ key data with a first  
4   password, writing ~~the said~~ encrypted key data to said storage medium,  
5   encrypting ~~a second~~ said first password with ~~said first~~ a second password, and  
6   writing ~~said second~~ the first encrypted password to said storage medium; and

7                   a read mode of decoding said ~~second~~ first encrypted password  
8   with said ~~second~~ password, obtaining said first password, and thereafter  
9   decoding ~~the said~~ encrypted key data with said first password.

1                   15.   (Cancelled)

1                   16.   (Currently Amended) The storage medium protecting method  
2   according to claim 1, said writing ~~the said~~ encrypted key data ~~step~~ is performed for  
3   all unit storage areas of ~~said the~~ storage medium when initializing ~~said the~~ storage  
4   medium.

1                   17. (Currently Amended) The storage medium protecting method  
2 according to claim 16, wherein said encrypting the data step comprises:

3                   a step of reading ~~the~~ said encrypted key data from ~~said~~ the storage  
4 medium;

5                   a step of decoding ~~said~~ the read encrypted key data with said  
6 password; and

7                   a step of encrypting the data with ~~said~~ the decoded key data.

1                   18. (Currently Amended) An encoding method for protecting data  
2 on a storage medium having a plurality of unit storage areas, comprising:

3                   a step of generating different random ~~key data~~ keys for each unit  
4 storage area of ~~said~~ the storage medium, encrypting ~~the~~ said different random key  
5 ~~data~~ keys with a password, and writing the encrypted key data keys to ~~said~~ the  
6 storage medium;

7                   a step of encrypting the data with ~~the~~ a different random key data  
8 corresponding to ~~said~~ a particular unit storage area to which the data, once  
9 encrypted is to be written, and writing the encrypted data to ~~said~~ the storage  
10 medium.

1                   19. (Currently Amended) A decoding ~~of protected~~ method for  
2 protecting data on a storage medium having a plurality of unit storage areas,

3 wherein different ~~key data is~~ keys are used for each unit storage area and the  
4 different ~~key data is~~ keys are encrypted with at least one password, comprising:

5 a step of reading the different encrypted ~~key data~~ keys from said ~~the~~  
6 storage medium;

7 a step of decoding the ~~said different~~ encrypted ~~key data~~ keys with  
8 said ~~the~~ at least one password; and

9 a step of decoding the data on said ~~the~~ storage medium with ~~the a~~  
10 particular decoded ~~key data~~ corresponding to ~~the a~~ particular unit storage area  
11 where the data, once encrypted have been read.

1 20. (Currently Amended) A storage medium data protecting  
2 method ~~of~~ for protecting data on a removable storage medium having a plurality of  
3 unit storage areas, comprising:

4 a step of generating random ~~key data~~ keys, encrypting said random  
5 ~~key data~~ keys with a password, and writing said ~~the~~ encrypted ~~key data~~ keys to the  
6 removable storage medium;

7 a step of encrypting the data on the removable storage medium with  
8 said ~~the~~ generated random ~~key data~~ keys, and writing said ~~the~~ encrypted data to the  
9 removable storage medium;

10 a step of reading said encrypted ~~key data~~ from the removable storage  
11 medium;

12 a step of decoding said encrypted ~~key data~~ with said password; and

13                   a step of decoding and reading the data on the removable storage  
14 medium with ~~said the~~ decoded encrypted key data,  
15                   wherein said random key data-generating step further comprises:  
16                   a step of generating different random ~~key data~~ keys for each of a  
17 plurality of unit storage ~~areas~~ area of the removable storage medium;  
18                   a step of encrypting each of said different random ~~key data~~ keys for  
19 said each of said plurality of unit storage ~~areas~~ area with said password; and  
20                   a step of writing each ~~said of the~~ encrypted key data keys to the  
21 removable storage medium,  
22                   wherein ~~said the~~ data encrypting step comprises a step of encrypting  
23 the data on the removable storage medium with a particular random key data  
24 corresponding to a ~~one of said plurality of~~ particular unit storage ~~areas~~ area to write  
25 the data, and  
26                   wherein ~~said the~~ data decoding step comprises a step of decoding the  
27 data on the removable storage medium with said decoded encrypted key data  
28 corresponding to a ~~one of said plurality of~~ said particular unit storage ~~areas~~ area  
29 where the data, once encrypted, have been read.

1                   21. (New)       A storage medium data protecting method of  
2 protecting data on a storage medium comprising:  
3                   a step of generating a random key, encrypting said random key with  
4 a password, and writing said encrypted random key to the storage medium;

5                   a step of encrypting the data with the generated random key, and  
6   writing the encrypted data to the storage medium;

7                   a step of reading said encrypted key from the storage medium;

8                   a step of decoding said encrypted key with said password; and

9                   a step of decoding the data on the storage medium with the decoded  
10   key,

11                  wherein said writing said encrypted random key to the storage  
12   medium comprises a step of encrypting said random key with each of a plurality of  
13   passwords, writing said encrypted random keys to the storage medium, and said  
14   step of decoding the encrypted key comprises a step of decoding said encrypted  
15   key with a designated password.

1           22.   (New)       A storage medium data protecting method of  
2   protecting data on a storage medium comprising:

3                   a step of generating a random key, encrypting said random key with  
4   a password, and writing said encrypted random key to the storage medium;

5                   a step of encrypting the data with generated random key, and writing  
6   the encrypted data to the storage medium;

7                   a step of reading said encrypted key from the storage medium;

8                   a step of decoding said encrypted key with said password; and

9                   a step of decoding the data on the storage medium with the decoded  
10   key,

11                wherein said writing said encrypted random key to the storage  
12 medium comprises a step of encrypting said random key with a first password,  
13 writing the encrypted random key to the storage medium, encrypting said first  
14 password with a second password, and writing the encrypted first password to the  
15 storage medium, and

16                said step of decoding the encrypted key comprises a step of decoding  
17 said encrypted first password with said second password, and obtaining said first  
18 password, and a step of decoding said encrypted key with said obtained first  
19 password.

1                23.    (New)            A storage medium data protecting apparatus for  
2 protecting data, comprising:

3                a storage medium having a plurality of unit storage areas; and

4                a control circuit for reading and writing the data from and to said  
5 storage medium,

6                wherein said control circuit has:

7                a write mode of encrypting, after generating a random key, said  
8 random key with a password, writing said encrypted random key to the storage  
9 medium, encrypting the data with the generated random key, and writing the  
10 encrypted data to the storage medium; and

11                   a read mode of decoding, after reading said encrypted key from the  
12 storage medium, said encrypted key with said password, and decoding the data on  
13 the storage medium with the decoded key,

14                   wherein said write mode has a mode of encrypting said random key  
15 with each of a plurality of passwords, writing said encrypted random keys to the  
16 storage medium, and

17                   said read mode has a mode of decoding the encrypted key comprises  
18 a step of decoding said encrypted key with a designated password.

1                   24.   (New)    A storage medium data protecting apparatus for  
2 protecting data, comprising:

3                   a storage medium having a plurality of unit storage areas; and

4                   a control circuit for reading and writing the data from and to said  
5 storage medium,

6                   wherein said control circuit has:

7                   a write mode of encrypting, after generating a random key, said  
8 random key with a password, writing said encrypted random key to the storage  
9 medium, encrypting the data with the generated random key, and writing the  
10 encrypted data to the storage medium; and

11                   a read mode of decoding, after reading said encrypted key from the  
12 storage medium, said encrypted key with said password, and decoding the data on  
13 the storage medium with the decoded key,

14                wherein said write mode has a mode of encrypting said random key  
15    with a first password, writing the encrypted random key to the storage medium,  
16    encrypting said first password with a second password, and writing the encrypted  
17    first password to the storage medium, and

18                said read mode has a mode of decoding said encrypted first  
19    password with said second password, and obtaining said first password, and a step  
20    of decoding said encrypted key with said obtained first password.

1                25.    (New)        A storage medium data protecting method of  
2    protecting data on a storage medium comprising:

3                a step of generating a random key, encrypting said random key with  
4    a password, and writing said encrypted random key to the storage medium;

5                a step of encrypting the data with the generated random key, and  
6    writing the encrypted data to the storage medium;

7                a step of reading said encrypted key from the storage medium;

8                a step of decoding said encrypted key with said password; and

9                a step of decoding the data on the storage medium with the decoded  
10    key,

11               wherein said writing encrypted key is performed for all unit storage  
12    areas of the storage medium when initializing the storage medium,

13               and wherein said encrypting the data step comprises:

14               a step of reading said encrypted key from the storage medium;

15 a step of decoding the read encrypted key with said password; and  
16 a step of encrypting the data with the decoded key.

1 26. (New) A storage medium data protecting apparatus for  
2 protecting data, comprising:

3 a storage medium having a plurality of unit storage areas; and

4 a control circuit for reading and writing the data from and to said  
5 storage medium,

6 wherein said control circuit has:

7 a write mode of encrypting, after generating a random key, said  
8 random key with a password, writing said encrypted random key to the storage  
9 medium, encrypting the data with the generated random key, and writing the  
10 encrypted data to the storage medium; and

11 a read mode of decoding, after reading said encrypted key from the  
12 storage medium, said encrypted key with said password, and decoding the data on  
13 the storage medium with the decoded key,

14 and wherein said write mode has a mode of performing to write  
15 encrypted key for all unit storage areas of the storage medium when initializing  
16 the storage medium,

17 and wherein said write mode has a mode of reading said encrypted  
18 key from the storage medium; decoding the read encrypted key with said  
19 password, and encrypting the data with the decoded key.

1                   27.   (New)       A storage medium data protecting method of  
2   protecting data on a storage medium comprising:

3                   a step of generating a random key, encrypting said random key with  
4   a password, and writing said encrypted random key to the storage medium;

5                   a step of encrypting the data with the generated random key, and  
6   writing the encrypted data to the storage medium;

7                   a step of reading said encrypted key from the storage medium;

8                   a step of decoding said encrypted key with said password; and

9                   a step of decoding the data on the storage medium with the decoded  
10   key,

11                  wherein further comprising:

12                  a step of decoding, after reading said encrypted key from the storage  
13   medium, the said encrypted key with an old password designated by a user; and

14                  a step of writing, after encrypting said decoded key with a new  
15   password designated by said user, the encrypted key to the storage medium.

1                   28.   (New)       A storage medium data protecting apparatus for  
2   protecting data, comprising:

3                   a storage medium having a plurality of unit storage areas; and

4                   a control circuit for reading and writing the data from and to said  
5   storage medium,

6                wherein said control circuit has:

7                a write mode of encrypting, after generating a random key, said  
8 random key with a password, writing said encrypted random key to the storage  
9 medium, encrypting the data with the generated random key, and writing the  
10 encrypted data to the storage medium; and

11              a read mode of decoding, after reading said encrypted key from the  
12 storage medium, said encrypted key with said password, and decoding the data on  
13 the storage medium with the decoded key,

14              wherein said write mode further comprises a mode of decoding, after  
15 reading said encrypted key from the storage medium, the said encrypted key with  
16 an old password designated by a user, and writing, after encrypting said decoded  
17 key with a new password designated by said user, the encrypted key to the storage  
18 medium.